GDPR SCUOLA
LO STAFF TECNICO DEL DIRIGENTE

Analisi del rapporto Clusit 2021 sulla sicurezza ICT in Italia

A cura di Giacomo Lunardon, responsabile Servizi Tecnici Istituto Statale "A. Monti" di Asti e "CIS Controls Volunteer"

Puoi scaricare la versione integrale del rapporto alla pagina clusit.it/rapporto-clusit

---

Analisi dei principali attacchi

Nel 2020 si sono contati 1871 attacchi informatici ufficialmente riconosciuti, con un +12% rispetto al 2019 e una media di 159 attacchi al mese (con una netta crescita degli attacchi di tipo "Cyber Espionage/Sabotage/Warfare").

La tipologia di attacco varia a seconda degli obiettivi dei cybercriminali, che adottano tecniche diverse a seconda degli obiettivi.

Il settore "Healthcare" ha subito danni maggiori dai "ransomware" per fini estorsivi, mentre quello "Education/Research" ha visto come protagonisti le incursioni informatiche finalizzate al furto di dati (soprattutto nei casi di centri di ricerca medica legati allo studio dell'emergenza Covid-19).

Il maggior numero di attacchi è comunque quello di tipo "Multiple Target" tendente ad un'azione a più vasto spettro, che sfrutta le maggiori vulnerabilità in funzione della "superficie di attacco" dei sistemi informatici.

Altrettanto interessante è l'analisi degli strumenti e dei metodi di cybercrime utilizzati, che svariano dal classico "malware" al "phishing", dall'attacco "DDoS" allo sfruttamento delle "CVE".

La crescita percentuale di maggior rilievo si è verificata tuttavia nel settore del "Phone Hacking" (azione volta ad ottenere l'accesso al telefono cellulare intercettando le telefonate o rubando i messaggi informatici in esso contenuti) e del "SQL Injection" (azione volta ad ottenere l'accesso ai database utilizzando trasmissioni di richiesta dati attraverso il web, appositamente studiate per questo scopo).

Vale la pena considerare i tipi di malware maggiormente sfruttati dagli specialisti del cybercrime, che si avvalgono soprattutto dei “ransomware” (che codificano i dati presenti sui computer e li decifrano solo dietro pagamento di riscatto), dei programmi “criptominer” (che utilizzano i computer come basi di calcolo delle criptovalute), dei sistemi di “botnet” (che coordinano reti di insospettabili computer trasformandoli in sorgenti di attacco organizzato nei confronti di server o reti di vario genere).

A completamento di quanto appena elencato, una buona percentuale di attacchi (che varia a seconda dei target) viene messa a segno con tecniche non chiaramente identificate.

Attacchi a tema Covid

Il rapporto Clusit dedica anche un capitolo particolare agli attacchi a tema “Covid-19”, che nel 2020 sono stati 188 (circa il 10% del totale), realizzati soprattutto in primavera, con evidenti obiettivi di spionaggio, e organizzati al fine di colpire nel modo più rapido possibile un grande numero di obiettivi in parallelo.

Considerando l’emergenza ancora in atto, appare evidente come l’attenzione nei confronti di questi fenomeni debba rimanere costante ed elevata.

L’impatto degli attacchi

Non è sempre facile quantificare la gravità degli attacchi, in quanto i parametri che si possono considerare per esprimere un impatto “medio”, “grave” o “basso” sono piuttosto soggettivi e non formalmente codificati.

Più in generale, la valutazione dovrebbe basarsi su definizioni standard, che trovano espressione concreta nelle definizioni “DoCRA” (www.docra.org), e sono riassunte organicamente nel documento CIS Security Risk Assessment Method (www.cisecurity.org/white-papers/cis-ram-risk-assessment-method).

I malware più rilevanti secondo l’indagine Fastweb

Gli esperti del “Security Operations Center” di Fastweb hanno aggregato e anonimizzato i dati derivanti dalle anomalie create dai vari malware, individuando complessivamente circa 220 “famiglie”, tra le quali spicca “Andromeda”, software malevolo e modulare in grado di sfuggire alle analisi all’interno di macchine virtuali, e programmabile al fine di scaricare ulteriori programmi sui computer infettati.

I professionisti del cybercrime si avvalgono di un “arsenale informatico” che prevede l’utilizzo di altri virus, tra i quali ricordiamo “QSnatch”, “Mirai”, “Nivdort”, “Virut”, “Murofet” ed altri ancora.

Altro aspetto interessante dell’indagine Fastweb riguarda gli attacchi “DoS” (Denial of Service), tecnica diffusa a livello mondiale volta a provocare l’interruzione dei servizi di un singolo server o di una rete di computer.

Il tipico attacco “DoS” viene attuato nei confronti di un sito web, al fine di interromperne il funzionamento per eccesso di traffico.

Se pur non particolarmente diffusi nei confronti delle P.A., gli attacchi “DoS” subiti dal settore “Government” rappresentano comunque il 14% del totale.

L’obiettivo degli hacker in questo caso viene raggiunto più velocemente con le tecniche di “amplificazione” del traffico DNS e NTP, che produce nei confronti del server attaccato un traffico da 30 a 70 volte superiore a quello inizialmente utilizzato dall’attaccante.

Attacchi ransomware nel 2020 in Italia

Sono passati cinque anni circa dalla diffusione del primo “ransomware”, noto come “WannaCry”, in grado di criptare i files più comunemente utilizzati dalle suite di produttività (testi, fogli di calcolo, presentazioni), al fine di estorcere denaro (criptovaluta) per restituire nuovamente alla vittima la versione leggibile dei dati.

Con il tempo queste tecnologie di tipo “criptoworm” sono migliorate, agendo anche sulle copie di backup e trasferendo i file dei dati direttamente ai cybercriminali in formato leggibile (con il fine estorsivo ulteriore di divulgazione delle informazioni rubate).

Sovente gli attacchi di questo genere vanno a segno attraverso i messaggi di posta elettronica impropriamente aperti o non riconosciuti come pericolosi dai programmi antivirus.

Tuttavia possono verificarsi intrusioni anche attraverso porte e servizi disponibili (ad esempio RDP), e utilizzando siti modificati ad arte in grado di distribuire questi sistemi di cifratura criminale.

Indubbiamente le recenti necessità di “smart working” hanno aperto nuove porte ai criminali informatici che, sfruttando l’esposizione dei sistemi informatici alla connettività esterna, hanno visto crescere le opportunità di accesso alle reti di aziende e P.A.

Tra i “ransomware” più diffusi ricordiamo “Dharma”, “Phobos”, “Maze”, “Avaddon”, “AKO” ed anche una variante denominata con tragica ironia “CoronaVirus”.

Fenomeno di probabile origine italiana è quello della diffusione via email di una finta App spacciata come “Nuova App Immuni” che, una volta scaricata ed avviata, presenta una mappa della diffusione del Covid nel mondo, mentre procede indisturbata nel lavoro di cifratura dei file sul computer della vittima: l’obiettivo finale, come è facile immaginare, è l’estorsione di denaro per riottenere l’accesso al dispositivo colpito.

Sicurezza email

Il fenomeno Covid ha sicuramente influito sulla diffusione dell’utilizzo della posta elettronica, e di pari passo sull’incremento dei messaggi a contenuto pericoloso realizzati ad arte per carpire informazioni ed inviare malware di vario genere.

La pandemia ha dato lo spunto ai cybercriminali per mettere in atto le azioni di “phishing”.

Il grande numero di comunicazioni circolanti sul web, email incluse, ha offerto la possibilità di diffondere tra le molte informazioni lecite, numerosi messaggi falsi delle più svariate tipologie (dal finto licenziamento, alla finta raccolta fondi), provenienti dai più svariati e falsi mittenti: MEF, OMS, sanità pubblica, poste, banche, finti App store.

Anche la diffusione di malware allegati alla posta elettronica ha permesso l’utilizzo sia di nuove tecniche basate sull’esecuzione di codici malevoli, sia di “vecchi trucchi” legati alle macro-formule, entrambi inseriti e distribuiti nei documenti di Office allegati alle email.
Non meno importante - e sempre difficile da intercettare come pericoloso - è il messaggio di posta che contiene un link, più o meno credibile, in grado di portare il ricevente su siti illegali che replicano fedelmente l’aspetto dei siti ufficiali, con lo scopo evidente di carpire utenze e password delle vittime.

Stato della cybersecurity nell’Italia del sud

Lo studio realizzato dall’Università di Bari e da Exprivia S.p.A. ha coinvolto un campione di 304 tra aziende ed enti, evidenziando un livello di alfabetizzazione informatica medio-alto,

ma anche una notevole frammentazione di tipologia settoriale in ambiti aziendali di piccole dimensioni.

Una percentuale piuttosto alta (il 55,6%) non mette in atto azioni di verifica sulla sicurezza di software/servizi forniti da terze parti, e non presta particolare attenzione ai termini di adesione e sottoscrizione ai servizi cloud.

È interessante osservare come una buona percentuale del campione (il 41,2%) ammetta di non essere in grado di difendersi dagli attacchi informatici, e quasi l'intero campione (il 95,2%) ritenga utile la formazione in materia di sicurezza informatica, sintomo evidente che le aziende stanno cambiando la loro percezione sull'argomento.

Attività e segnalazioni della Polizia Postale

Il "Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche" (CNAIPIC), analizzando i dati relativi agli attacchi sia nei confronti delle grandi infrastrutture che dei singoli enti, individua una condotta riconducibile al crimine organizzato a livello transnazionale.

Gli eventi di cybercrime presi in considerazione dimostrano inoltre che gli attacchi sono organizzati da esperti del settore provvisti di notevoli risorse.

Il CNAIPIC nel 2020 ha censito ben 509 attacchi (con una crescita del 246% rispetto al 2019), ma l'azione di contrasto della Polizia Postale ha concluso importanti indagini, tra le quali ricordiamo le operazioni "Data Room" e "GLAAKI".

Financial cybercrime e truffe online

A causa dell'effetto pandemico, nel 2020 è cresciuto il numero di utenti che hanno utilizzato i servizi online messi a disposizione delle banche, e di pari passo sono cresciute le azioni malevole volte ad insinuarsi tra clienti ed istituti di credito con l'impiego di finti siti clonati e utilizzando le varianti del "phishing" denominate "Vishing" (simulazione di una chiamata proveniente dal call center dell'istituto di credito) e "Smishing" (invio sul telefono di un messaggio che induce a fidarsi di un link ricevuto in precedenza).

Fenomeni di "BEC e CEO Fraud" si sono verificati parallelamente al diffondersi dell'evento pandemico, assumendo l'aspetto di vere e proprie frodi commerciali nell'ambito medico e farmaceutico (acquisto di mascherine e/o di prodotti medicali).

Sono state effettuate indagini anche su segnalazioni di truffe online messe in atto da soggetti che vendevano mascherine, guanti e igienizzanti in modo contraffatto e fraudolento.

Non sono mancate neppure le false raccolte fondi poste in essere attraverso siti web apparentemente riconducibili ad ospedali, o accreditate con falsi patrocini di Istituzioni ed Enti Pubblici.

La Polizia Postale, nella sua attività di contrasto delle azioni criminali che utilizzano le tecnologie informatiche e il web, monitora numerosi eventi illegali controllando i cyberterroristi, la divulgazione di notizie false, l'utilizzo di falsi account per scopi illegali, la diffusione di contenuti estremisti e radicalizzanti, l'odio religioso e razziale.

Altrettanto importante è il contrasto alla pedopornografia online, all'adescamento online, al cyberbullismo e ai reati commessi attraverso i social network.

Internet of Things (IoT)

Il report Clusit analizza il fenomeno della diffusione dei dispositivi che, con il loro hardware, possono connettersi ad altri simili o compatibili, potendo anche collegarsi alla rete.

Questi vengono comunemente individuati come "IoT" ovvero "Internet of Things", apparecchiature sempre più diffuse anche a livello domestico, costituite da veri e propri mini computer configurabili per il controllo remoto e programmabili per la gestione del funzionamento dell'apparecchio nel quale vengono installati.

La loro rapida diffusione non è sempre collegata a una serie adeguata di studi sulle problematiche di sicurezza e vulnerabilità che si possono generare durante il loro utilizzo.

Le notizie sui "bug" dei sistemi operativi e dei software non sono mancate, e a livello mondiale molti dispositivi (ad esempio le telecamere di sorveglianza o "baby monitor") hanno presentato gravi carenze di sicurezza (il protocollo "iLnkP2P" è risultato carente in termini di crittografia e di accesso senza autenticazione).

Anche la prima versione del sistema "VxWorks" è risultata carente per ben 11 punti differenti (lacuna poi colmata con i più recenti aggiornamenti).

I ricercatori di Palo Alto Networks hanno evidenziato in uno studio statistico che molti dispositivi di “medical imaging” negli USA funzionano con sistemi operativi obsoleti, e che, più generalmente, il 98% del traffico inviato dai dispositivi IoT non è crittografato.

Il fatto più preoccupante è sicuramente la diffusione di queste gravi lacune di sicurezza, concentrate soprattutto nelle apparecchiature medicali meno recenti ma comunque ancora diffusissime.

Tra il 2019 e il 2020 sono diventate di dominio pubblico diverse vulnerabilità, sfruttate da una nuova variante del malware botnet “Mirai”, in grado di colpire i sistemi di presentazione wireless WePresent WiPG-1000 e le TV LG Supersign, e il malware “Silex”, in grado di ricercare ed identificare dispositivi IoT scarsamente protetti, basati su Unix o Linux, rendendoli inutilizzabili.

Inoltre alcuni cybercriminali hanno utilizzato attacchi di tipo hijacking verso i sistemi di controllo degli accessi agli edifici intelligenti, utilizzandoli per lanciare attacchi DDoS.

Come considerazione generale, le falle nel mondo “IoT” sono spesso dovute all’uso di credenziali di autenticazione di default, alla possibilità di accedere in modo non autenticato ai dispositivi, alla gestione remota tramite protocolli di connessione non sicuri, alla mancata cifratura delle comunicazioni, alla commistione e alla mancanza di segregazione delle reti, al mancato aggiornamento del firmware, all’utilizzo di sistemi operativi obsoleti e alla mancanza di uno sviluppo software coordinato e controllato in maniera sicura.

La grande diffusione degli oggetti “IoT” e la loro natura estremamente eterogenea, rende questo ambito di applicazione molto soggetto alle vulnerabilità e, pur riconoscendo l’indubbia utilità nel campo dell’automazione, vale la pena sottolineare come questi dispositivi siano presenti ovunque: webcam, router, sistemi di presentazione wireless aziendali, telecamere di sicurezza, baby monitor, campanelli intelligenti, sistemi di videoregistrazione, sistemi medicali, stampanti, sistemi UPS, dispositivi di rete, sistemi di videoconferenza, sistemi di controllo per ascensori e accesso agli edifici, sistemi di controllo dell’irrigazione, sistemi di climatizzazione, grandi elettrodomestici, antifurti, ecc.

Analizzando i dati messi a disposizione da FortiGuard Labs, si dimostra come gli attacchi nell’ambito “Operation Technology” vengano messi in atto dai cybercriminali al fine di bloccare il funzionamento di apparecchiature e macchinari di grandi aziende (inviando pacchetti dati su porte particolari al fine di generare un DoS), accedere ai file e ai dati sui server attraverso la vulnerabilità Laquis SCADA, tentare l’esecuzione di comandi remoti sui

sistemi embedded QNX, creare disservizi nei sistemi di automazione industriale agendo sulla vulnerabilità ABB IDAL.

Le minacce del web e le truffe online

Come più volte segnalato in precedenza, l'evento pandemico ha "aperto la porta" a numerose attività cybercriminali, diffuse su più canali.

Da marzo 2020 queste azioni malevole sul web hanno subito un notevole incremento, sfruttando molte tecniche in grado di ingannare anche gli utenti esperti.

Tra i vari sistemi adottati per truffare in rete si possono citare le azioni spam e phishing, le pagine di phishing specifico su software Adobe, le finte finestre che danno finti allarmi di infezione virus per ottenere il clic, pagine contenenti iframe malevoli, pagine di phishing contenenti script all'interno del body, pagine di phishing generico generate da email, re-indirizzamento del traffico su pagine indesiderate, refresh delle pagine con indirizzamento su siti pericolosi, inserimento di codice associato a siti malevoli, spam generico, tecniche di scam per indurre le vittime a dare informazioni o denaro, finte pagine di login, ecc.

Come potrebbe evolversi la situazione nel 2021?
I cybercriminali sono in grado di sfruttare velocemente ogni occasione per attuare i loro attacchi, ma ora dovremo confrontarci con un altro cambiamento significativo, dovuto allo sviluppo della metodologia "intelligent edge" e all'introduzione del 5G.

Probabilmente queste nuove tecnologie saranno prese di mira, e verranno utilizzate a loro volta per colpire altre vittime, sfruttando le sempre crescenti prestazioni hardware dei sistemi informatici e la velocità di trasmissione introdotta dal 5G.

Per prevenire scenari particolarmente nefasti si dovranno considerare come probabili: l'utilizzo dei "trojan" evoluti con lo scopo di colpire l'edge, gli attacchi swarm edge-enabled, il ricorso al social engineering, la crescente diffusione dei dispositivi IoT domestici, i malware sfruttati a scopo di riscatto.

Guerra informatica minaccia imminente

Le minacce e gli eventi di cybercrime fino ad ora valutati possono inevitabilmente portare alla domanda più ovvia: "Gli esperti di sicurezza informatica cosa possono fare per affrontare queste minacce?".

Domanda più che lecita, che nella sezione dedicata del rapporto Clusit trova numerosi spunti di analisi e relativi commenti sui dati statistici raccolti.

Circa la metà dei professionisti del settore ICT ritiene che la “guerra informatica” sia una minaccia concreta, eppure circa un terzo ammette di non avere una strategia in atto per mitigare questo rischio.

Lo studio pubblicato da Clusit ha preso in considerazione un campione di oltre 6700 addetti del settore in tutto il mondo, intervistando un campione rappresentativo che passa dalle PMI alle grandi aziende quotate in borsa.

Come primo dato emerge il timore che gli attacchi ransomware possano aumentare nei prossimi mesi, così come sale al 46% l’opinione di coloro che temono per la loro infrastruttura un attacco critico che possa interrompere l’attività lavorativa, e circa un terzo ammette che se la propria attività fosse colpita sarebbe disposto a pagare il riscatto ai cybercriminali.

Parallelamente, i professionisti della sicurezza ICT concordano che la strategia migliore per aumentare gli investimenti in questo settore sia legata essenzialmente ad una più efficace metodologia di comunicazione, una più efficace condivisione delle conoscenze e l’adozione di un linguaggio meno tecnico.

Quest’ultimo aspetto “comunicativo” auspica la possibilità di far comprendere agli organi decisionali (dirigenti, CDA) quali siano i rischi concreti e le potenziali conseguenze di un attacco informatico ai sistemi aziendali.

Il problema maggiore del settore della sicurezza informatica nel suo complesso è la carenza cronica di personale competente ed esperto: i professionisti interpellati concordano sul fatto che siano necessarie competenze diversificate (75%), e confermano che una maggiore “neurodiversità” possa rendere il settore più forte e più paritario nei confronti degli hacker (73%).

La sicurezza dei dati nel cloud

Il tema della conservazione e della gestione dei dati nel cloud è sempre più pressante, in quanto un numero crescente di aziende e P.A. adotta questa soluzione sia per l’attività lavorativa quotidiana, sia per l’archiviazione permanente dei dati.

L'adozione di questa soluzione è spesso dovuta a due aspetti fondamentali, ovvero la limitazione delle risorse economiche da indirizzare in questo ambito, e la scarsa o nulla disponibilità di personale preparato per affrontare le problematiche tecniche derivanti da una gestione dei dati completamente attuata con risorse proprie.

Anche il cloud risulta vulnerabile al cybercrime, registrando statisticamente incidenti di sicurezza causati soprattutto dai tentativi di "phishing" e dai soliti "ransomware".

Una percentuale minore ma comunque importante è dovuta alla cosiddetta "fuga accidentale di dati".

Dai dati statistici rilevati quasi la metà degli eventi non ha generato conseguenze gravi, ma nel 28% dei casi chi ha subito l'attacco ha dovuto sostenere spese non previste per correggere le lacune rilevate.

I professionisti della sicurezza, intervistati a proposito della sicurezza dei dati nel cloud, lamentano lacune di personale da adibire a questi controlli, carenza di budget e scarsa esperienza nell'ambito del cloud stesso.

Le misure più comunemente adottate sono la crittografia, il controllo accesso utenti e la formazione del personale addetto.

Più in generale, gli intervistati affermano di voler rimuovere quanti più dati sensibili dal cloud, ma questa scelta porta a chiederci dove e come verranno conservati questi dati.

L'analisi statistica ha evidenziato come le grandi aziende siano più propense al "declouding", mentre le piccole e medie imprese, probabilmente per motivi economici e organizzativi, pare non seguano la stessa tendenza.

Come dato generale, si osserva come circa il 27% del budget dedicato alla sicurezza informatica venga speso per l'ambito cloud, ma anche sotto questo aspetto le piccole imprese si differenziano rispetto alle grandi per l'impatto percentuale dell'aumento di budget (solo il 17% delle piccole imprese ha aumentato il budget per la sicurezza), elemento che evidenzia l'elevata incidenza del rapporto costo/benefici di queste misure, al di sotto del quale non è evidentemente possibile scendere.

Dal punto di vista statistico, gli incidenti più comuni sono riconducibili a casi di "phishing", "ransomware", perdita accidentale dei dati, attacchi mirati al cloud, compromissione

dell'account, furto da parte di addetti e hacker, ma nel complesso non vi sono grandi differenze statistiche tra piccole e grandi aziende, anche se queste ultime hanno subito tendenzialmente un numero maggiore di attacchi di tipo "phishing" e "ransomware".

Tra gli elementi da tenere in considerazione vi è la tempistica necessaria per riconoscere l'attacco e porre rimedio all'evento hacker.

In queste occasioni è risultato quasi immediato (in termini di poche ore) il rilevamento di un attacco "ransomware", mentre in caso di furto o perdita dei dati i tempi si sono allungati notevolmente.

Più in generale gli incidenti sono da imputare a un utilizzo "sovraesposto" dei dati.

La tecnica più comune per migliorare il controllo dei dati è basata sulla catalogazione e sul controllo di accesso da parte degli utenti.

Nei casi di perdita o furto dei file, le operazioni di individuazione diventano molto più veloci ed efficaci in termini di analisi di tempi e modalità dell'incidente informatico.

L'efficacia di queste "best practices" aumenta con l'utilizzo di software e hardware dedicati alle attività di backup e "file versioning".

Le misure di sicurezza più diffuse per il controllo dei dati in cloud prevede, nella maggior parte del campione statistico analizzato, l'uso della crittografia, il controllo e la formazione degli utenti e il backup dei dati.

Al fine di rendere ancora più efficaci queste misure, i maggiori player mondiali nell'ambito software offrono vari sistemi di controllo e accesso al cloud (Cloud Access Security Broker) per implementare al meglio le policy di sicurezza.

Merita maggiore attenzione lo studio statistico di Clusit per quanto riguarda il settore "Istruzione", che denuncia incidenti di sicurezza nel cloud per seguenti casi: attacchi di phishing (60%), compromissione dell'account (33%), ransomware o altri attacchi malware (27%).

Gli effetti principali di questi incidenti si sono concretizzati come segue: spese non pianificate per colmare le lacune di sicurezza (33%), abbandono dei clienti (10%), diminuzione della valutazione aziendale (9%).

I dati analizzati sottolineano come il settore “Istruzione” abbia presentato tempi di riconoscimento legati alla perdita accidentale di dati piuttosto elevati (giorni o settimane nel 93% dei casi), con tempi di ripresa talvolta molto lunghi (nel 33% dei casi).

Le organizzazioni educative comunque dichiarano di aver già provveduto (o pianificano di farlo) all’applicazione delle principali misure di sicurezza (backup cloud, controllo attività utente, diritti di accesso).

Business Continuity

Il report Clusit dedica anche spazio al tema “Business Continuity”, ovvero l’applicazione delle soluzioni di tecniche ed organizzative finalizzate a garantire la continuità dell’erogazione di un servizio.

Nel 2020 le organizzazioni hanno evidenziato la forte dipendenza dalla loro infrastruttura tecnologica, che deve essere in grado di affrontare attacchi informatici e violazioni della sicurezza.

Di conseguenza, gli aspetti di IT & Cyber Security e quelli di Business Continuity dovranno sempre più interagire con le funzioni di Security e Risk Management per garantire la salvaguardia dei sistemi informatici fisici e virtuali.

In sintesi, il contesto sempre più caratterizzato dai processi accelerati di digitalizzazione ed automatizzazione che stiamo vivendo non può che concretizzarsi in una stretta correlazione tra Information & Cyber Security e Business Continuity.